

### **REMARKS**

Claims 1-24 and 45-50 are presently pending. The Office Action mailed 3-17-08 rejects Claims 1-24 and 45-50 as unpatentable over Mitchell et al. (US 2003/0149661 A1) in view of Waters et al. (US 2002/0147600) per 35 USC 103(a). Claims 12-14 were rejected under 35 USC 103(a) as unpatentable over Mitchell et al. (hereinafter Mitchell) as modified by Waters et al. (hereinafter Waters), as applied to Claim 1, and further in view of Kipp (US 5,239,167).

By this Amendment, Applicant made a minor amendment to Claim 24 so that the limitation pertaining to the clearing house reads more similarly to the limitation set forth in Claims 46-48. No new limitations that were not already implied by the existing claims or the record were added. Applicant further argues in favor of the rejected Claims 1-24; 45-50. For the reasons set forth below, the present Application is submitted as properly defining an invention patentable over the prior art. Reconsideration, allowance, and passage to issue are respectfully requested.

### **INTRODUCTION**

The invention as claimed represents a paradigm shift in tokenless transaction systems. Namely, it's an entirely new notion that existing infrastructure, accounts, and so on, can be left substantially the same; and a separate remote database (which may be independent of a bank or other financial institution) may be used to maintain information for a user's existing financial accounts; and this database (which may be selectively modified by a user online in certain embodiments) may output specific account information as needed to the existing transaction infrastructure in response to biometric information. Consequently, existing transaction infrastructure, such as clearing houses, bank computers, merchant payment hosts, user accounts, and so on, can be left substantially the same. Furthermore, implementation of the system cannot be held hostage by refusal of financial institutions to adopt the system.

Various prior art has not experienced wide spread implementation, which is consistent with the fact that all of the art of record exhibit significant impediments to widespread implementation, as the systems of the art of record generally must be accepted by a plurality of independent entities, unlike the invention as claimed, which may be implemented without involvement of a bank, financial institution, or merchant payment host.

Hence, the paradigm shift in tokenless transaction systems, as provided by the invention as claimed, can be more fully understood with additional examples. For example, one embodiment within the scope of the present claims employs a remote user-configurable database to selectively deliver a financial account number to a charging terminal for the purposes of making a charge via the charging terminal. The charging terminal and network to which it is connected, including clearing houses, banking networks, hosts, and so on, may be pre-existing infrastructure that does not require substantial modification for implementation of certain embodiments disclosed herein. The charging terminal may charge the account number similar to how existing charges are made. This is entirely unlike Mitchell or Waters, which both use a database that is integrated with the charging infrastructure, such as clearing houses or merchant hosts.

Specific discussions of Waters and Mitchell and their applicability to the invention as claimed are provided near the end of this Amendment. Mitchell is discussed in more detail in Applicants proceeding Amendments C and D, which are herein incorporated by reference herein. In particular, see pages 26-33 of Amendment C, which sets forth various benefits of the invention as claimed over Mitchell. Such benefits of the invention as claimed over Mitchell also represent benefits over Waters, as discussed more fully below.

The examples discussed throughout this Amendment are not intended to be restrictive of the claims, but instead, they are intended to provide examples of certain embodiments falling within the scope of certain claims and examples of embodiments with benefits that are enabled by certain limitations (e.g., recited structure and/or function) of certain claims. Applicant requests that for the purposes of overcoming the prior art that the scope of the claims not be narrowed by anything written in Applicant's Remark sections of Amendments. If the scope of any claims are or have been narrowed by any of Applicant's remarks, Applicant

respectfully requests that the examiner indicate in writing which limitations of which claims have been considered to have been narrowed by language in Applicant's remarks.

### Rejections Under 35 U.S.C. 103(a), General Discussion

The invention is set forth in claims of varying scope. Claim 1 is illustrative:

1. A system for facilitating transactions comprising:
  - a charging terminal for charging an account based on an account number;
  - a scanner for obtaining biometric information; and
  - first means for employing said biometric information to provide said account number to said charging terminal, said charging terminal adapted to initiate charging said account upon or after being provided said account number by said first means.(Emphasis added.)

Note that device of Waters does not initiate charging an account after being provided an account number, but instead requires user input/approval of the transaction (e.g., Waters, [0022], lines 8-12 thereof) and further requires that the payment host further authenticate the transaction via the biometric data before the payment host initiates the transaction. Certainly, the payment device 18 of Waters does not initiate charging an account in response to receipt of an account number. Waters at most teaches use of a payment host to send transaction information to a payment device to obtain user approval before the payment host initiates the transaction, where the transaction infrastructure of Waters, including the payment host, has been modified to use biometric information and an accompanying identity lookup database.

Regarding Mitchell, as purportedly admitted in the present Office Action (Office Action p. 4, ¶2) any account number retrieved to the charging terminal of Mitchell would not be used to subsequently initiate a charge via the POS terminal as presently claimed. Hence, no charging terminal disclosed in Mitchell or Waters receives an account number in response to biometric information and then automatically uses that account number to thereafter initiate a charge (e.g., see Claims 1, 22, 45), such as via preexisting infrastructure. Note that any purported "first means" of Waters would require user participation or approval (Waters

[0022]; block 170 of Fig. 2B), and a user cannot be part of a means for rejection of the claims, as discussed more fully below.

The invention as claimed provides significant benefits over the art of record. These benefits, which are discussed more fully below, negate any suggestion that the invention is obvious in view of the art of record. For example, by using biometric information to retrieve an account number for use by preexisting transaction infrastructure, such as a clearing house, existing bank or credit card account, and so on, various benefits result. For example, there is no longer a need to modify existing transaction infrastructure, such as clearing houses, payment hosts, or bank accounts to enable the infrastructure to handle biometric information.

Unlike Waters and Mitchell, widespread use of an embodiment of the invention as claimed need not depend upon acceptance of the system by clearing houses, hosts, banks, and so on. Biometric information need not be proliferated among plural banks, merchant payment hosts, clearing houses, and so on, which could increase fraud exposure.

In addition, users can configure the first means (e.g., database) to retrieve any one of a number of different account numbers in response to different biometric information or combinations of biometric information instead of having to reapply at banks or other financial institutions for special accounts, and so on. In addition users can readily change associations as desired. Such significant benefits negate any suggestion that the invention is obvious in view of Mitchell or Waters, as discussed more fully below.

Accordingly, neither Waters nor Mitchell teach, disclose, or suggest the first means as recited in Claim 1 and certainly neither Waters nor Mitchell teach providing an account number to a POS for the purposes of charging the account number via a POS or other preexisting infrastructure. Waters simply forwards account information to the payment device of Waters to obtain user approval of a transaction and to enable a user to keep records of his charges (e.g., Waters. [0022]-[0023]); not to initiate a charge via the payment device. Waters uses the merchant payment host, which represents modified transaction infrastructure, to initiate a transaction after obtaining approval from the user and further authenticating the user by checking the biometric information associated therewith.

Furthermore, unlike Waters or Mitchell, the invention as claimed need not be implemented at a clearing house or merchant payment host and/or via a database in

communication with a clearing house or merchant payment host. In addition, implementation of the system does not require costly modification to an existing clearing house or merchant payment host or repetitive modification to different bank or charge card accounts, and the system does not require acceptance by associated clearing houses and banks.

Claim 15 as amended recites:

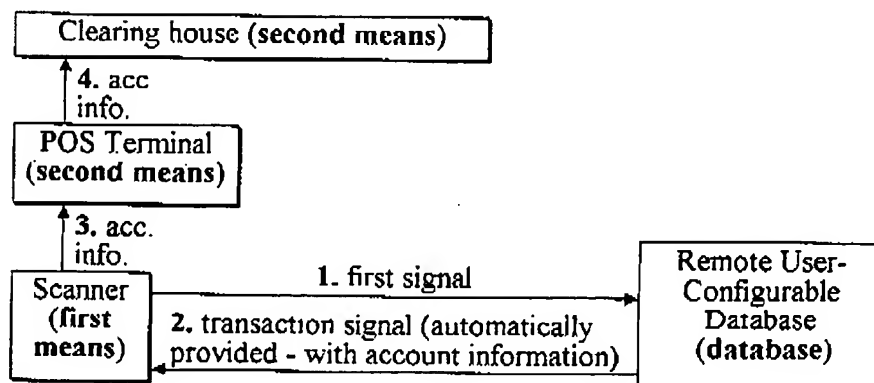
15. A system for facilitating a financial transaction comprising:

first means for measuring one or more biological characteristics of a user;

a database that is modifiable by a user of said system, wherein said database is adapted to select an account associated with said user based on said one or more biological characteristics and to provide a transaction signal in response thereto; and

second means for implementing a funds transfer to or from said selected account in accordance with said financial transaction in response to said transaction signal. (Emphasis added.)

The following simplified diagram, which based on diagrams in the Application, is shown for illustrative purposes:



The databases of Mitchell and Waters are not user modifiable, as it is unlikely (and not taught in Mitchell or Waters) for a user to be able to modify databases of clearing houses or merchant payment hosts. Instead, biometric information is obtained, and the databases are populated upon application of a user for a special financial account (e.g., Waters [0018];

Mitchell [0024]). Furthermore, the databases are connected with and may be considered a part of the clearing houses or merchant payment hosts (e.g., Waters [0010] p. 2, col. 1, ln. 15-17), despite whether the databases are shown in separate blocks, as the functionality of the databases is used directly by the clearing houses or merchant payment hosts (e.g., Mitchell [0023]; Waters [0021]). The databases of Mitchell and Waters do not operate independently or remotely from the clearing houses, merchant payment hosts, bank accounts, or other transaction infrastructure thereof.

The invention as claimed requires little or no modification to existing transaction infrastructure, such as the clearing house, bank or credit card accounts, and so on.

### **Rejections Under 35 USC 103(a), Specific Discussion**

**Regarding Claim 1**, the above-identified Office Action maintains many of the previous rejections made in Office Actions of 6-27-07 and 10-10-06. Nevertheless, the present Office Action of 3-27-08 admits that Mitchell does not teach use of a charging terminal adapted to initiate a charge after being provided an account number retrieved via biometric information (Office Action p. 4, ¶2).

In rejecting Claim 1, the present Office Action references Figs. 1-2 and [0017]-[0024] of Waters to further suggest that Waters teaches a system 10 comprising a payment host 20 coupled to a payment device 18 and biometric input device 14 for transmitting acquired biometric data to an identity lookup database 24 and initiating a financial transaction in response to the received result from the database by transmitting the data to a banking network 30.

However, the position that the payment device 18 of Waters initiates a financial transaction by transmitting data received from a database to a banking network 30 is in error. Instead, the merchant payment host 20 (not the payment device) initiates the transaction by transmitting the data to a banking network 30 via EFT messaging (e.g., Waters [0023], p. 3, col. 2) only after user authorization is obtained by the merchant payment host 20 via the payment device 18. Hence, the payment device 18 is not a charging terminal as taught in the present Application, but the payment device 18 of Waters instead merely provides biometric

information and authorization information to a clearing house (merchant payment host) for transaction authentication.

The payment device 18 must first obtain approval of a transaction, as the user must determine whether to proceed with a transaction (e.g., Waters [0022]). This is not an automatic step, as such a determination would require user input, which is not automatic, and a user cannot be part of a means, as discussed more fully below. The payment device 18 is not used to initiate a transaction, but instead the merchant payment host 20 initiates the transaction. Even if the payment device 18 did initiate a transaction, it would be in response to user authorization or approval [0022] and not in response to or upon receipt of the account number from the merchant payment host 20 as claimed. In Waters, the account number is transmitted via an account message from the merchant payment host 20 to the payment device 18 (e.g., Waters [0021]) for an entirely different purpose, i.e., to obtain user authorization (e.g., Waters [0022]) and not to use the payment device to initiate a transaction in response to receipt of the account number as claimed.

Furthermore, the need to obtain additional user input in Waters (e.g., Waters [0022]) represents a significant disadvantage, which is overcome by the invention as claimed. The need to obtain additional user input requires additional network messaging, which may slow the networks and further delay shopping lines. Accordingly, the invention as claimed is not obvious in view of Waters and/or Mitchell, or surely a system that can provide a charging terminal with an account number ready to be charged would be shown in the art of record due to the significant advantages afforded thereby. Neither Waters nor Mitchell, taken alone or in combination teach, disclose, or suggest the invention as presently claimed in Claim 1.

Note that after the authentication step discussed in Waters [0023], second sentence, the account number is not transmitted back to the payment device to initiate charging, but instead, the merchant payment host 20 initiates charging via an EFT signal to the banking network (e.g., Waters [0023], p. 3, col. 2). The payment device 18 of Waters is not initiating the transaction as the term "initiating" is used and claimed in the present Application.

The Office Action further suggests that it would have been obvious to combine Waters and Mitchell to provide a separate identity lookup database for managing each and every biometric data that is linked to particular account information (Office Action p. 4, ¶4).

However, this is not taught in Waters. Waters does not teach use of a separate database. Furthermore, it would not be obvious to provide a separate database to feed preexisting transaction infrastructure with account numbers for charging, or surely this would be shown in the art due to the significant advantages afforded thereby. Such advantages include minimizing the need to modify existing infrastructure; eliminating the need for various financial institutions, such as banks and credit card companies to adopt the system; enabling embodiments employing user configurable databases, where a user can assign different account numbers to different biometrics at will, and so on, as discussed more fully below.

Instead, the database 24 of Waters is integrally connected with the merchant payment host 20 and might as well be included in the same box. For example, the database is specifically maintained by the host 20 (e.g., Waters [0010], p. 2, col. 1, ln. 15-17). The database 24 and merchant payment host 20 of Waters must intercommunicate (e.g., [0021]-[0023] of Waters). The database 24 is certainly not independent or remote from the host 20 of Waters (also see Claim 48), which may be considered a clearing house in that it interfaces with the banking network 30 to facilitate payments.

Since Claim 1 is not taught, disclosed, or suggested by Mitchell, the corresponding dependent Claims 1-14 are also necessarily not taught, disclosed, or suggested by Mitchell, Waters, or the combination thereof. Nevertheless, the following discussion of the rejections pertaining to each claim further exemplifies how each claim further distinguishes over the art of record.

**Regarding Claim 2**, the Office Action cites [0023]-[0024] of Mitchell in suggesting that Mitchell discloses a charging terminal that includes a credit card or ATM terminal, and wherein the account number provided to the charging terminal includes a credit card number and corresponding expiration date or an ATM number and a corresponding PIN.

However, this position is in error. Nowhere does Mitchell disclose retrieval of a PIN to a charging terminal (POS) based on biometric information, and certainly neither Mitchell nor Waters, nor the combination thereof teach, disclose or suggest retrieval of a PIN to a charging terminal for the purposes thereafter of initiating charging a corresponding account via the charging terminal. Mitchell at most suggests printing a statement or transmitting a



confirmation of the transaction to the originating terminal (e.g., Mitchell [0023], last two sentences. Any suggestion that printing a statement or transmitting a confirmation of a transaction to a terminal discloses transmitting a PIN to a charging terminal for the purposes thereafter of making a charge requires hindsight, as this is not taught in Mitchell or Waters. Waters teaches at most transmitting a transaction message to a charging terminal to obtain user approval of a proposed transaction, where the user's biometric information must be subsequently authenticated before a charge can be initiated by the clearing house, called the host 20 in Waters (e.g., Waters [0021]-[0023]). This is entirely different than transmitting an account number and/or a PIN to a charging terminal to initiate a charge. Waters would have no reason to transmit the PIN to the payment device, as this is not needed for the host to obtain user approval of the transaction, and since account information is transmitted to the payment device of Waters for entirely different purposes: not to initiate a charge via a terminal or preexisting infrastructure.

In general, use of hindsight, which involves reading into "the prior art the teachings of the invention in issue," is inappropriate to reject the claims despite whether the claims are rejected under 35 USC 102 or 103. See *Monroe Auto Equipment Co. v. Heckethorn Mfg. & Sup. Co.*, 332 F.2d 406, 412 (1964). Note that, with simpler cases, as here, the danger increases that "the very ease with which the invention can be understood may prompt one to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher." See *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999), abrogated on other grounds by *In re Gartside*, 203 F.3d 1305, 53 USPQ2d 1769 (Fed. Cir. 2000).

**Regarding Claim 3**, the Office Action rehashes previous rejections in view of Mitchell (Office Action p. 2-4). However, such previous rejections are in error as discussed in Applicant's Amendments C and D. In addition, the Office Action does not explain how any of the art of record (e.g., Mitchell or Waters) teaches, discloses, or suggests use of a user-modifiable database.

As discussed in Amendment C, the database in Mitchell is not user modifiable, as it is unlikely (and not taught in Mitchell) for a user to be able to modify clearing house databases.

Similarly, the database of Waters is a merchant payment host database in that it is managed by the merchant payment host (e.g., Waters [0010] p. 2, col. 1, ln 15-17). It is unlikely (and not taught in Waters) for a user to be able to modify payment host databases. In fact, it is widely known that when outside entities access various bank databases or clearing house databases, such access is termed "a database break-in" or "account information was hacked." Obviously, such databases as disclosed in Waters and Mitchell are not taught as being user-modifiable, but instead, the databases are modified by the banks or other financial institutions at the time a user applies for a special financial account (e.g., Mitchell [0055] and [0051; Waters [0020]).

The Office Action further suggests that Mitchell discloses means for automatically selecting, based on biometric information, an account from plural accounts ([0017]-[0018] and [0049]) (Office Action p. 3, ln. 1-3). However, the selection of accounts disclosed in Mitchell clearly involves manual user manipulation of "controls" to select an account via an EFTPOS [0049], wherein the account is associated with a biological identifier. This does not anticipate or suggest automatic selection of an account from among plural accounts based on biometric data. Instead, the biometric data in Mitchell is employed to authenticate a user for access to an account or to process a transaction, such as by determining approval of a transaction (e.g., bottom portion of [0034]). Biometric data in Mitchell not used to perform the account selection as claimed.

While Mitchell appears to disclose using different fingerprints to access (not select) different accounts (last portion of [0008]), an account associated with a given fingerprint is not automatically selected. Instead, Mitchell requires the user to manipulate controls to select accounts, as discussed in the last sentence of [0050] of Mitchell and in [0049], second sentence.

Hence, neither Waters nor Mitchell, taken alone or in combination, teach, disclose, or suggest the invention as recited in Claim 3.

**Regarding Claim 4**, the Office Action cites [0049] of Mitchell in suggesting that Mitchell discloses second means for enabling a user to control which account number is selected by the first means as recited in Claim 4 (Office Action p. 3, ln. 4-5). However, neither Mitchell nor Waters even disclose the first means, as discussed above. The Office

Action suggests that the controls referred to by Mitchell in [0049] are sufficient to disclose the second means recited in Claim 4.

However, note that the first means of Claim 4 includes a database, as recited in parent Claim 3. The controls referred to by Mitchell in no way enable a user to control the database to affect which account number is selected by the database in response to or based on biometric information. Instead, the user actually makes the selection by manually picking an account. This is entirely different than the user modifying a database or otherwise affecting how the database uses specific biometric information to automatically select an account, as claimed. Note that any account selection in Mitchell would not be automatic (e.g., see parent Claim 3) as would be required to reject Claim 4.

Mitchell instead discloses use of POS controls to enable a user to select one or more accounts associated with a biological identifier that the user provides ([0049]). Hence, in this case, Mitchell is employing the biological identifier to authenticate a user to use a particular account, which may be used instead of a signature. Mitchell does not even disclose *selection* of accounts via biometric data, rather Mitchell discloses enabling *access* to accounts or charging an account via use of biometric data. Certainly, Mitchell in no way teaches, discloses, or suggests enabling a user to readily configure or to control how accounts are automatically selected based on certain biometric input.

Note that the present Application teaches use of a user-accessible remote database 32 (Fig. 1 of the present Application), whereby account selection rules may be configured by a user, such as via a PC 42. Note that neither Waters nor Mitchell does disclose the remote database 32, which would enable a user to configure account-selection rules. Instead, the clearing house of Mitchell and the merchant payment host of Waters manage biometric data (e.g., Waters [0010] p. 2, col. 1, ln. 15-17), and biometric data must be transmitted to the clearing house, bank, or merchant payment host to proceed with a transaction unlike the invention as claimed (e.g., Mitchell [0064], [0023], [0034]; Waters [0022]-[0023]). See also [0044] of Mitchell, where a customer applies to MasterCard to use their fingerprint.

Consequently, the user cannot readily change his registered biometric information or parameters associated therewith. Any such change would be implemented by the bank or

credit card company after the user tediously contacts the clearing house and each bank to re-register the biometric information.

As an addition example, Mitchell does not anticipate enabling a user to configure the system to automatically select, for example, one card in response to biometric information pertaining to the left eye and another card in response to biometric information pertaining to the right eye, and to readily change the configuration as desired (e.g., parent Claim 3 recites user-modifiable database). In addition, Mitchell does not disclose enabling a user to, for example, automatically select an account via a combination of a thumb scan and an iris scan (e.g., p. 13, ln. 24-27 of the present Application). In addition, Mitchell does not anticipate enabling a user to configure the system to allocate, for example, charges above a certain dollar amount to a card with a higher limit (p. 12, ln. 16-19 of the present Application). Hence, the invention as claimed in Claim 4, and the various embodiments enabled via the limitations claimed therein, are not anticipated by and are not obvious in view of Mitchell or Waters or the combination thereof.

**Regarding Claim 5**, the Office Action cites [0050]-[0051] of Mitchell to suggest that Mitchell further discloses some scheme for prioritizing accounts sufficient to anticipate Claim 5 (Office Action p. 3, ln. 8-9).

However, nowhere in Mitchell, and certainly not in [0050]-[0051], does Mitchell disclose a user-modifiable database that enables a user to prioritize plural accounts. And certainly, none of the art of record anticipates establishing priorities for accounts of a user, where an available account with the highest priority is automatically selected for transmission of the account number to a charging terminal to initiate a charge.

Instead, Mitchell discusses use of a display to enable a customer to choose between commonly used credit card or charge card companies, e.g., MasterCard, Visa, etc. approved by a particular merchant [0050]. This in no way teaches, discloses, or suggests prioritization of accounts and certainly does not suggest use of a database that is adapted to enable a user to prioritize plural accounts, as claimed. Instead, Mitchell teaches selection of a credit card or a charge card company.

Certainly, Mitchell does not disclose prioritizing accounts, where an available account is automatically selected for retrieval to a charging terminal as claimed. Merely providing a list of merchant-approved credit card or charge card companies as taught in Mitchell is entirely different than enabling a user to prioritize or sort accounts so that an available account with the highest priority is automatically selected for retrieval to a charging terminal. Any suggestion that the credit card or charge card companies or associated accounts may somehow be prioritized by a user or merchant in Mitchell or Waters would require hindsight, as such suggestion does not appear in Mitchell or Waters. Accordingly, rejection of Claim 5 is further improper. Furthermore, any such prioritization would not result in automatic selection by a mechanism (first means) that automatically retrieves the corresponding account number to a charging terminal.

Recall that Mitchell does not teach use of biometric information to select an account, but rather to access a single account. Furthermore, any selection of an account taught in Mitchell would not be automatic as claimed (e.g., grandparent Claim 3), but would require manipulation of controls as taught in [0049] of Mitchell, and the user would have to be part of the means, which is inappropriate. Consequently, Mitchell does not anticipate the invention as claimed in Claim 5.

Regarding Claim 6, the Office Action suggests that Mitchell further discloses software (320 in Fig. 3 of Mitchell) that enables a user to trigger automatic selection of an account based on which type of biometric information or combination of biometric information that the user provides [0049] (Office Action p. 3, ln. 10-12).

However, Applicant does not find a reference numeral 320 in Fig. 3 of Mitchell, and no mention of any such software can be found in Mitchell. The database of Mitchell is not taught as having software that enables a user to trigger automatic selection of an account based on which type of biometric information that a user provides. Instead, [0049] of Mitchell discusses manual selection of an account via controls on a reader, not via software in a database. Any account selection is performed by the user, not software, and any such selection would be manual, not automatic.

Nowhere does Mitchell suggest that a reader or other device could enable, for example, a user to trigger selection (let alone automatic selection) of an account based on whether the user provides biometric information pertaining to facial scan, an iris scan of one eye, a combination of a thumb print and a voice scan, etc., as enabled by one embodiment according to Claim 6.

The features recited in various claims, such as Claim 6, are particularly beneficial, enabling users to associate different body parts or other biometric information or combinations thereof with different account numbers. This may eventually obviate the need for a user to carry any card, including a drivers license, as the biometric information may enable retrieval of photographs, license numbers, and so on, to an appropriate terminal as needed for a particular application.

Furthermore, if a user believes that a thief has stolen biometric information pertaining to his thumb, for instance, the user may access the user-modifiable database to disable associations between thumb biometric data and credit cards or other financial accounts. The user might instead employ associate a given account with a combination of biometrics, e.g., the thumb and the index finger. Such significant benefits suggest that the invention is not obvious, especially considering that the invention has not been implemented or disclosed in the art of record.

**Regarding Claim 7**, the Office Action suggests (Office Action p. 3, ln. 12-14) that Mitchell discloses fourth means for providing transaction information to the first means as claimed in Claim 7. However, since Mitchell does not disclose the first means as indicated above, Mitchell necessarily does not disclose sending transaction information thereto.

Note that, as discussed above, neither Mitchell nor Waters disclose a user-modifiable database as claimed. Furthermore, note that neither Mitchell nor Waters disclose a first means or a database that employs biometric information to provide an account number to a charging terminal for the purposes of initiating a charge via the charging terminal.

Waters at most discloses a system that transmits an account message to a payment device to obtain user approval of the transaction (e.g., Waters [0022]) before a host or clearing house initiates a transaction, where initiation of the transaction by the host or clearing

house occurs after the user's biometric information is compared to a signature received in a transaction message sent from the payment device (e.g., Waters. [0022]-[0023]) Hence, Waters in no way suggests that an account number is sent to the charging terminal to initiate a transaction. Note that the payment device, merchant payment host, and so on do not represent pre-existing transaction infrastructure to which an account number is delivered for charging. Instead, the transaction infrastructure of both Mitchell and Waters must be modified, which is problematic, as discussed more fully below. The significant disadvantages of Mitchell and Waters in light of the invention as claimed mitigate in favor of patentability of the present claims.

**Regarding Claim 8**, the Office Action suggests (Office Action p. 3, ln. 14-17) that Mitchell further discloses fifth means ([0053]-[0056]) for enabling a user to specify selection rules or selection criteria based on transaction information that dictate which account is selected by the first means.

However, [0053]-[0056] discuss an embodiment wherein a user must apply to different financial institutions to be able to use different biometrics for different accounts. This in no way suggests use of a user-modifiable database. In addition, this in no way teaches a mechanism for enabling a user to specify selection criteria based on transaction information as claimed. Any selection of accounts in Mitchell would be by the user, and would not be automatic selection by the database based on pre-established rules set up by a user via a user-configurable database, and would not be based on transaction information per se, as this is not taught or suggested in Mitchell. Mitchell is entirely different than the invention as claimed, and Mitchell in no way anticipates the limitations of Claim 8. Mitchell clearly does not show modifiable selection rules usable by the database thereof for dictating account selections. Mitchell merely shows user selection of accounts. No set of modifiable selection rules or criteria can be found in Mitchell.

Mitchell also discloses associating different biological identifiers with different accounts (e.g., Mitchell [0053]). However, this in no way teaches, discloses, or suggests specifying selection rules. Instead, Mitchell at most teaches association of different biological identifiers with different accounts so that different accounts can be manually (not

automatically) selected via controls as taught in [0049]. For example, a user may submit one finger to a fingerprint reader and then select that corresponding account associated with the biological identifier. Use of additional fingers for different accounts would in no way suggest or teach a mechanism for enabling a user to specify selection rules that dictate which account is automatically retrieved to a charging terminal, and even if selection rules existed in Mitchell, the selection rules obviously would have to be preestablished. Recall that Mitchell does not even disclose retrieval of account information to the charging terminal for the purposes of initiating a charge. Clearly, Mitchell neither teaches, discloses, nor suggests use of selection rules that dictate or control *automatic* selection of an account, let alone selection of an account based on transaction information or biometric information.

Unlike Mitchell, an embodiment according to Claim 8 might enable a user to automatically charge dinners to a Discover<sup>(R)</sup> card; to charge airfares to an American Express<sup>(R)</sup> card; and to charge gasoline to a MasterCard<sup>(R)</sup>. Alternatively, a user may specify that transactions above a certain dollar amount be charged to one account, and transactions below a certain dollar amount be charged to another account (as discussed, for example, on page 12, lines 16-25 of the present Application). Such functionality may yield significant previously unanticipated results in enabling users to organize, categorize, charge, and account for various expenses. Such significant results suggest that the invention is not obvious, as discussed more fully below. Otherwise, Mitchell, Waters, or other art would teach or anticipate such advantages, functionality, and configurability.

**Regarding Claim 9**, the Office Action suggests (Office Action p. 3, ln. 18-22; p. 4, ln. 1-3) that Mitchell further discloses sixth means for limiting selection of account numbers as claimed in Claim 9. Specifically, the Office Action suggests that the POS terminal of Mitchell will have a card reader to read the magnetic strip on a credit or debit card, and that this information is linked to a keypad on an EFTPOS remote terminal that enables the customer to enter a PIN if required. The Office Action further suggests that in the case of a credit card transaction, the user may push the button marked "credit" so that the information from the card and the customer's PIN if required is transmitted to a clearing house.



However, note that such limitations purportedly shown in Mitchell would necessarily not be included in a database, let alone a user-modifiable database, as would be required to reject Claim 9.

Furthermore, even if Mitchell discloses what the Office Action suggests, use of a card reader to relay credit card information and PIN to a clearing house in no way anticipates employing transaction type information to limit automatic selection of account numbers to only those account numbers that are compatible with the transaction type. With reference to page 12, ln. 12-30 of the Application, an example of transaction type information might include information indicating a transaction is beyond a certain dollar amount or information indicating that the charge is a credit card charge. Nowhere does Mitchell teach use of such information to limit selection of account numbers as claimed.

Note that in the present Application, the selection of account numbers may be performed, for example, by the remote database 32 of Fig. 1. Mitchell does not disclose any module that is similar to the remote database 32 of Fig. 1 of the present Application.

Note that Mitchell suggests that a customer must choose (i.e., the database of Mitchell does not include means for choosing), via the POS, from among commonly used merchant-approved credit card or charge card companies. Generally, in Mitchell, any selection of account numbers is user-controlled ([0049]), while access is enabled via a biometric identifier. Nowhere does Mitchell disclose a mechanism for selectively limiting selection of account numbers as recited in Claim 9. Any mechanism for selecting account numbers would be the user himself/herself, which should not be considered a mechanism, and account selection would not be considered automatic.

Hence, Mitchell does not disclose automatic selection or retrieval of account numbers and certainly does not disclose use of transaction type information to limit automatic selection of account numbers. Rather, Mitchell implies that a user must use controls to select which account to use [0049]. Accordingly, Mitchell does not anticipate the invention as claimed in Claim 9.

Regarding Claim 10, the Office Action (Office Action p. 4, ln. 3-7) suggests that Mitchell further discloses a database [0018] that is remotely accessible to a user and that the

database includes means for authenticating the user before allowing the user to alter selection rules associated with user accounts ([0019]-[0021]) maintained by the database.

However, the database discussed in Mitchell is a database at the clearing house, where the biometric identifier and transaction is processed ([0023], [0034], [0052] first sentence, etc.). The database at the clearing house clearly cannot be readily edited or configured by a user, and the database of Mitchell certainly is not taught as being remotely accessible via the Internet. Instead, the user must, for example, apply to MasterCard to use their fingerprint ([0055] at p. 4, col. 2). Alternatively, the user applies to the bank ([0024], at p. 2, col. 2). Hence, the user cannot readily edit their biometric information via a particular mechanism of Mitchell, and certainly cannot alter account selection rules via a database of Mitchell.

The requirement that the user apply at each bank or credit card company is particularly problematic, as discussed more fully below. For example, if the user has multiple cards, the user must perform a tedious process to change biometric information at each bank or credit card company. Furthermore, Mitchell would result in the undesirable proliferation of credit card information among banks, credit card companies, and clearing houses. Note that the clearing house database discussed in Mitchell likely obtains biometric data from the credit card companies, since the biometric data must be processed by the clearing house ([0014], [0023] at p. 2). Hence, the user would not have direct access to the clearing house database to alter account-selection rules. User access to clearing house databases is unlikely, since clearing houses are well known to closely guard access to their databases.

Furthermore, nowhere does Mitchell show a database, let alone a user-modifiable database, that communicates with a means for authenticating a user before allowing a user to alter the database or selection rules associated with accounts of a user. Any authentication discussed in Mitchell is for the purposes of charging an account; not for the purposes of enabling a user to alter selection rules implemented by a database.

Hence, Mitchell does not anticipate the invention or any of the limitations as recited as claimed in Claim 10.

**Regarding Claim 11**, the Office Action suggests (Office Action p. 5, ln. 3-5) that Mitchell further discloses seventh means (clearing house; [0051]-[0052]) for automatically providing transaction information to a charging terminal.

However, note that neither Mitchell nor Waters disclose automatic retrieval of an account number to a charging terminal as recited in Claim 1, and consequently, neither Mitchell nor Waters, nor the combination thereof teaches the invention of Claim 11. Note that Mitchell does not disclose, for example, automatic retrieval of transaction amount, transaction type, and so on, to a charging terminal (p. 12, ln. 6-7 of the present Application), but instead teaches that an approval or declined indication is provided to the charging terminal [0034]. Any receipt printed for the customer would not necessarily include an account number, as such information is often omitted from receipts to avoid fraud. Even if the receipt discussed in Mitchell (e.g., [0052], last ¶) of Mitchell did include an account number, the transaction would have already been completed. Consequently, the account number would not be used to subsequently make a charge via the charging terminal. Furthermore, neither does Waters suggest delivering an account number to a charging terminal to initiate a charge, as discussed above, but instead delivers a message to a payment device to obtain user approval of a transaction.

**Regarding Claim 15**, Applicant finds no specific rejections in the present Office Action of 3-17-08. Certainly neither Mitchell nor Waters anticipate a user modifiable database, let alone a database that is adapted to select an account number based on one or more biological characteristics as recited in Claim 15. Accordingly, Claim 15 should be allowable in view of the art of record.

Note that Examiner's previous rejections (made in a previous Office Action of 10-10-06) to a previous version of Claim 15, maintain Mitchell discloses a payment system (Fig. 1 of Mitchell) that includes first means for measuring one or more biological characteristics (fingerprint reader); second means for selecting an account (controls along with arrow keys); and third means for implementing a funds transfer ([0052]).

Note, however, that use of controls and arrow keys to select an account (e.g., [0049]) would not constitute selection performed by a mechanism or means as claimed in Claim 15, as

a user cannot be a mechanism in a claim, as forcefully stated, for example, in *In re Prater*, 415 F.2d 1393, 1398 (CCPA 1969). See also *Default Proof Credit Card System, Inc. v. Home Depot U.S.A., Inc. et al.*, No. 05-1069 (Fed. Cir. 2005), where the Court determined that "...arguments that the structure corresponding to the 'means for dispensing' can entail human (or 'merchant') participation or a human being manually operating an apparatus, are equally misplaced."

Instead, the controls and arrow keys require manual user input. Even in the embodiment of Mitchell that employs the "fingerprint credit card," account selection is not performed by a mechanism, but requires user participation. The user must still inform the vendor, i.e., select, whether the user will use a credit, debit, or fingerprint card, etc. ([0050], last portion). Accordingly, Mitchell does not teach, disclose, or suggest a mechanism for selecting accounts as claimed in Claim 15. Hence, Mitchell clearly does not anticipate the invention of Claim 15.

Since Claim 15 is not taught, disclosed, or suggested by Mitchell, the corresponding dependent Claims 16-24 are also necessarily not taught, disclosed, or suggested by Mitchell. Nevertheless, the following discussion of the rejections pertaining to each claim further exemplifies how the claims distinguish over the art of record.

**Regarding Claim 16**, the Office Action (Office Action p. 5, ln. 6-12) suggests that Mitchell further discloses means for providing a first signal (good scan) based on one or more biological characteristics, said first signal acting as an authorization signal, an authentication, and an account-selection signal, the second means providing the transaction signal based on the first signal (acceptance), and wherein the second means (controls and arrow keys) does not require participation of a clearing house.

Note, however, that Claim 16 recites that the database does not require participation of a clearing house. Controls and arrow keys certainly do not represent a database. Nowhere does Mitchell or Waters disclose a database that does not require participation or a clearing house, also called a merchant payment host in Waters

Note that the second means as claimed facilitates implementing a funds transfer from a selected account in response to a transaction signal. Controls and arrow keys would require

user participation, and a user cannot be part of a mechanism used to reject a claim, as discussed above. Accordingly, controls and arrow keys alone, without a human, cannot be used to facilitate implementing a funds transfer, and controls and arrow keys do not teach, disclose, or suggest any limitations recited in Claim 16.

Even if controls and arrow keys alone could be considered a means for facilitating implementing a funds transfer as claimed, the so-called first signal, i.e., good scan obtained in Mitchell is certainly not taught as being a signal that is provided to a database, let alone a user-modifiable database that can provide a transaction signal to "arrow keys," i.e., the second means.

Furthermore, note that the manual controls and arrow keys suggested by the Office Action as representing the second means cannot possibly represent the second means, since, for example, arrow keys cannot receive a transaction signal as would be required. See Claim 15, which states "...said database providing said transaction signal to said second means..."

Furthermore, the biological identifier of Mitchell is not used to select an account, but instead is used as an authentication signal to access an account. Note that in Mitchell, account selection is apparently performed by a user who employs controls to select an account, as discussed in [0049] of Mitchell, instead of via the biological identifier. Mitchell does not specifically teach or suggest use of a biometric to choose specifically between user accounts, and certainly not between accounts maintained by a single database, and certainly not a user-modifiable database.

As discussed above, and elaborated upon further in this paragraph, Mitchell does not disclose the second means for selecting an account, as any selection in Mitchell would inappropriately require incorporation of a user in the second means. Hence, Mitchell necessarily does not disclose use of the second means to provide a transaction signal based on the first signal (good scan) as claimed in Claim 16. In addition, in rejecting the parent Claim 15, the Office Action suggests that the second means of Claim 15 corresponds to controls and arrow keys of Mitchell. However, clearly, the controls and arrow keys of Mitchell, which must be controlled by a user, cannot provide (by themselves) a transaction signal based on the first signal (good scan) as the rejection suggests, and even if they did, this is not what Claim

16 recites, i.e., Claim 16 does not recite that the second means provides a transaction signal as the rejection maintains.

Mitchell would require manual user participation, and Mitchell would require the user to be part of the second means. However, a human should not generally be used as a "means" to reject a claim, as forcefully stated, for example, in *In re Prater*, 415 F.2d 1393, 1398 (CCPA 1969).

Hence, neither Mitchell nor Waters anticipate the invention as claimed in Claim 15 and certainly not Claim 16 and should not be used for rejection thereof.

**Regarding Claim 17**, the Office Action suggests (Office Action p. 5, ln. 13-16) that Mitchell further discloses that the second means includes a database ([0017]-[0018]) for selectively outputting account information contained in the transaction signal based on the first signal.

However, it is virtually impossible for controls and arrow keys (see rejection cited in the Office Action, p. 5, ln. 11) to include a database. Recall that in rejecting the parent Claim 15, Examiner suggests that the controls and arrow keys of Mitchell represent the second means. Control and arrow keys cannot themselves output account information or receive a transaction signal and cannot themselves include a database. Consequently, the purported second means of Mitchell would not anticipate Claim 17.

Furthermore, note that Claim 17 actually recites a database that is adapted to selectively output account information to a charging terminal of the second means via a transaction signal in response to a first signal. The current rejection is inapplicable to Claim 17. In addition, any signal containing account information provided to a charging terminal by Mitchell would not be used to initiate a charge via the charging terminal.

Furthermore, note the database referred to in [0017]-[0018] of Mitchell does not output account information contained in a transaction signal as claimed in Claim 17. Any account information, which is used internally in the clearing house of Mitchell, would be information stored in the database and not contained in a transaction signal. Mitchell does not teach retrieving account information in a transaction signal and then outputting the account information as claimed.

Nowhere does Mitchell teach mechanisms for using biometric information as a database key to enable a database to simultaneously authenticate a user and to select an account *and* to provide account information, such as an account number and PIN, in response to the account selection and user authentication. Instead, account selection is performed via user input [0049], and an approved or declined indication, not account information, is returned from the clearing house in Mitchell.

Furthermore, similar rejections based on Waters would also be inapplicable, as Waters does not teach a user-modifiable database, and Waters does not teach that the database thereof can communicate with a second means, such as a charging terminal, but instead, the merchant payment host 20 of Waters communicates with the payment device 18. Note that Claim 17 recites, in part, that the database outputs account information to a charging terminal. This is neither shown in Waters nor Mitchell.

**Regarding Claim 18**, the Office Action (Office Action p. 5, last ¶, i.e., ln. 17-24) suggests that Mitchell further discloses a database that includes a user-configurable account list that enables a user to control which account is automatically selected by the second means in response to the first signal (good scan; [0024]-[0025]).

However, Mitchell does not teach that the account list is user configurable or editable. No controls or mechanisms are provided for enabling a user to readily change entries in the account list without having to reapply or apply to different financial institutions (e.g., Mitchell [0024]), which can be prohibitive.

Furthermore, as discussed above, the account selection in Mitchell is apparently not performed by a mechanism, but by a user [0049]. Note that since Mitchell does not disclose *a mechanism or means for* account selection, such as the database as claimed, Mitchell necessarily does not disclose enabling a user to configure automatic account selection behavior as claimed in Claim 18.

While Mitchell apparently stores information in a machine-readable form (Mitchell [0023]), but Mitchell does not teach, disclose, or suggest a mechanism to allow the user to

readily configure the information. At most, Mitchell teaches that a user can select accounts (Mitchell [0049]) but not modify the database.

As discussed above, a bank or clearing house is unlikely to allow a user to modify or configure the bank's databases. Instead, a user would have to apply (e.g., Mitchell [0044] last portion), and then the bank or MasterCard would then edit their own databases accordingly, if they accepted the user. This in no way teaches, discloses, or suggests, user modification of the databases. Even if Mitchell did disclose user modification of the clearing house databases, which could be a security concern, the database discussed in Mitchell lacks any mechanism to enable a user to change which account is automatically accessed or selected in response to a given "good scan." Accounts are not even automatically accessed. Hence, Mitchell does not anticipate or suggest Claim 18.

**Regarding Claim 19**, the Office Action further suggests (Office Action p. 6, ¶1) that Mitchell includes means for identifying a user (biometric reader and card/check reader; [0033]) before enabling the user to access or configure information that is stored via the database.

However, Mitchell does not even disclose a user-configurable database, and Mitchell cannot possibly disclose a means for identifying a user before enabling the user to access or configure the database.

Furthermore, note that the computer discussed in [0033] of Mitchell is used to make Internet-based purchases ([0064]-[0083]) and not to store or configure information in the database as claimed. Nowhere does Mitchell teach, disclose, or suggest that the computer is equipped to enable a user to configure or access information stored in the database, which in Mitchell is apparently maintained at the clearing house, banks, or credit card companies in communication with the clearing house (e.g., Mitchell [0023], [0051]).

The biometric reader and card/check reader of Mitchell is apparently used to authenticate a user for a financial transaction and to implement the transaction. Mitchell in no way suggests that the biometric reader and card/check reader are used to identify a user before allowing the user to configure or access a database. In Mitchell, the user does not have access to the database. Instead, the database is used internally by the clearing house or by the



clearing house in communication with one or more banks or credit card companies. See Fig. 4 of Mitchell, for example, where the user input is limited to a transaction entry 100, which may involve submitting to a fingerprint scan via a fingerprint reader (Fig. 1 of Mitchell). Submitting a transaction entry is entirely different than modifying, accessing, or configuring a database. Hence, Claim 19 is not anticipated by and is not obvious in view of Mitchell.

Regarding Claim 20, the Office Action suggests (Office Action p. 6, ¶2) that Mitchell further discloses a means for enabling a user to predetermine account selection rules for accounts listed in the database ([0055]).

However, Mitchell does not teach use of account selection rules for accounts listed in any database and certainly does not teach user-modification of account selection rules. Instead, account selection is performed manually by the user via relatively tedious interaction with a POS (Mitchell [0049]-[0050]).

Modification of any account selection rules, which are not taught in Mitchell, would require user access to a clearing house or bank database and would require the user to have database-modification privileges. This is undesirable and unlikely. Any modification to a clearing house or bank database would be performed by the clearing house or bank at the discretion of the clearing house or bank, and not by the user, as made clear in [0055] of Mitchell. Hence, Claim 20 is not anticipated by and is not obvious in view of Mitchell.

Note that [0055] of Mitchell merely suggests that a user must apply to different financial institutions to be able to use different biometrics for different accounts. This in no way suggests a database with user-modifiable account selection rules. Instead, this illustrates a grave problem with Mitchell, which is overcome by the invention as claimed. Namely, the system of Mitchell presupposes that different financial institutions will adopt the system. However, institutional reluctance to adopt the system, for whatever reason, may be prohibitive. Hence, the system is "captive" to the will of participating institutions. This has undoubtedly inhibited the widespread use of systems, such as Mitchell.

This significant problem is overcome by certain embodiments enabled by structure and/or function recited in one or more of the present claims. For example, use of a separate user modifiable database to provide an account number to preexisting transaction

infrastructure based on biometric information obviates these problems, such as the need to proliferate biometric information among financial institutions or the need for such institutions to accept the system. Hence, the invention cannot possibly be considered obvious in view of the past art.

Regarding Claim 21, the Office Action suggests (Office Action p. 6, ¶3) that Mitchell further discloses a terminal that is positioned remotely from a POS that enables a user to predetermine account selection rules (EFTPOS remote in Fig. 1 of Mitchell) as claimed.

However, Claim 21 recites a terminal or computing device that is adapted to enable a user to modify information in a database that is positioned remote from a point of sale. Mitchell does not disclose a user modifiable database and certainly does not disclose a computing device for modifying the database or selection rules, as thoroughly established above and throughout this Amendment.

Furthermore, the so-called EFTPOS remote of Mitchell is for entering a transaction (100 of Fig. 4), which would occur at a POS, unlike the invention as claimed in Claim 21. One should not be confused by the term “remote terminal” as implying that the terminal is located separately from the POS. Instead, Mitchell confirms that the EFTPOS remote is located at a merchant store, i.e., at a POS (e.g., Mitchell [0085], first sentence).

Furthermore, as the name implies, the EFTPOS is an Electronic Funds Transfer (EFT) Point-Of-Sale (POS) terminal, and consequently, is positioned at a POS. The EFTPOS remote terminal is called “remote” likely because it is coupled to the card reader and not incorporated therein (as shown in Fig. 1 of Mitchell). The assembly of devices of Fig. 1, including the EFTPOS remote, are apparently co-located at a POS and Mitchell does not suggest otherwise.

Nevertheless, even if the EFTPOS remote were positioned remotely from a POS, Mitchell still does not teach, disclose, or suggest use of the EFTPOS to modify a database or to enable a user to configure or predetermine account selection rules as claimed. Selecting an account to charge via an EFTPOS terminal is entirely different than predetermining account selection rules. Hence, Mitchell does not teach, disclose or suggest a terminal positioned remotely from a point-of sale that enables a user to predetermine account selection rules or to

otherwise modify a database, such as claimed in Claim 21. Accordingly, Claim 21 is not anticipated by and is not obvious in view of Mitchell.

Certain embodiments within the scope of one or more of the present claims may enable a user to configure the system at home or via other remote terminal away from the POS. This may result in potentially significant benefits, especially in terms of reduced checkout lines at merchant outlets, such as stores, restaurants, and so on. The system of Mitchell apparently requires the navigation of potentially complicated or intimidating user interfaces at a POS, which may be particularly problematic, as discussed more fully below.

**Regarding Claim 22**, the Office Action suggests (Office Action p. 6, ¶4) that Mitchell further discloses means for employing the first signal (good scan) to authenticate (credit database matching process and resulting signal) the user before providing the transaction signal to the third means ([0052], clearing house).

However, note that Claim 22 does not recite a third means. Applicant assumes that the Office Action is referring to the second means. Note that the mechanism for implementing a funds transfer in Mitchell is apparently the clearing house (Mitchell [0052]; [0023], last portion). Consequently, the "good scan" of Mitchell is not employed to authenticate the user before providing the transaction signal to the clearing house as claimed. In the system of Mitchell, processing of the biometric data (authentication) would have to occur at the POS to teach authenticating a user before a transaction signal is sent to the clearing house. Instead, processing of biometric data clearly occurs at the clearing house in Mitchell (e.g., [0014], [0023]). Hence, Claim 22 is neither anticipated by nor is obvious in view of Mitchell. Note that determining whether a reader has made a good scan or a bad scan is not equivalent to authentication.

**Regarding Claim 23**, the Office Action suggests (Office Action, p. 6, ¶5) suggests that Mitchell further discloses means for storing information pertaining to one or more biological characteristics of a user when the means for employing fails to authenticate a user [0051].

However, Mitchell does not disclose this. Merely checking whether a scan of a biological identifier is a good scan or a bad scan, as discussed in [0051] of Mitchell, is entirely different than storing biological characteristics when a mechanism fails to authenticate a user. Furthermore, determining if a scan is good or bad is not equivalent to authenticating a user, but instead determines if the scan is sufficiently clear [0051]. Hence, Mitchell does not teach, disclose, or suggest a mechanism for storing biometric data associated with a failed or fraudulent authentication attempt.

If Mitchell had anticipated such, then Mitchell surely would have suggested that storing of information pertaining to failed authentication attempts could be used to thwart fraud as discussed in the present Application. See the fraud-alert system, as discussed, for example, on p. 8, ln. 15-25 of the Application. Such significant results are not taught or suggested by any mechanism or combination of mechanisms in Mitchell.

Hence, Mitchell does not state or suggest that biological characteristics are stored *when* authentication fails as recited in Claim 23, and Claim 23 is neither anticipated by nor is obvious in view of Mitchell.

**Regarding Claim 24**, the Office Action suggests (Office Action, p. 6, last ¶, p. 7, first ¶) that Mitchell discloses third means that includes a credit card, charge card, and/or Automated Teller Machine (ATM) charging module, and wherein the transaction signal includes a selected credit card, charge card, or ATM card number associated with said user and any relevant pins or dates ([0052]).

However, Claim 24 does not recite a third means. Application assumes that the Office Action intends to refer to the second means when citing the third means.

Note that the database in Mitchell is not positioned remotely from a clearing house (e.g., Mitchell [0051], ln. 11, [0023]), but instead, is included in the clearing house. Mitchell certainly does not disclose the invention as claimed, and neither does Waters, as discussed more fully below.

Furthermore, note that the clearing house as discussed in [0052] of Mitchell does not include a credit card, charge card, and an ATM charging module and, consequently, does not anticipate Claim 24.

In addition, note that the charging modules of Mitchell (Fig. 1 of Mitchell) do not implement a funds transfer in response to a transaction signal provided by a mechanism (second means) for automatically selecting an account. For example, Mitchell does not teach, disclose, or suggest a database, such as the database 32 of Fig. 1 of the present Application, that provides a card number (transaction signal) to a charging module for the purposes thereafter of making a charge via the number. Claim 24 is neither anticipated by nor is obvious in view of Mitchell.

In summary, nowhere does Mitchell teach, disclose, or suggest use of biometric information to automatically select or retrieve account information from a database to a *charging* terminal, which thereafter initiates a charge. Neither does Waters. Any account information provided to a terminal in Waters is to obtain user approval of a transaction and/or to enable a user to keep records of charges made (such as via a written record, perhaps a check book or ledger) (Waters [0023], p. 3, col. 2).

Furthermore, note that embodiments of Mitchell and Waters generally require a user to manually select an account for charging, such as via a controls [0049] and a user interface [0050], which requires, for example a user to press an "OK" button. Mitchell generally neither discusses automatic *selection* of an account based on predetermined rules nor discusses automatic retrieval of the selected account information to a conventional terminal.

In addition, note that neither Waters nor Mitchell disclose remote or independent databases. Instead, for example, the database of Waters communicates with and is maintained by the clearing house (Waters [0010] p. 2, col. 1, ln. 15-17, and Fig. 1) , i.e., the merchant payment host in Waters (e.g., juxtapose Fig. 1 of Waters and Fig. 4 of Mitchell with reference to [0084] of Mitchell). Accordingly, neither Waters nor Mitchell discloses a remote or independent database that does not require modification to a clearing house or merchant payment host.

While the lookup database 24 of Waters is depicted in a different box than the merchant payment host 20, i.e., clearing house, of Waters, Waters does not teach the database 24 as being geographically separate or remote from the host. Instead, the implementation discussed in Waters suggests that the database would be integrated on the same computer as the host 20. The host 20 and database 24 appear to be separate for functional discussion

purposes. This is because the identity lookup database 24 is maintained by the merchant payment host (Waters [0010] p. 2, col. 1, ln. 15-17), and Waters discusses no need and no advantages of geographically separating the database 24 from the host 20. In fact, geographically separating the database 24 from the host 20 would slow transaction processing due to delay over any communications link connecting the entities 20, 24. The mere depiction of a different box for the identity database does not teach, disclose, or suggest that the database is positioned remotely from a clearing house.

**Regarding Claim 45,** Applicant finds no specific rejection thereto, but instead a compilation of previously made rejections of other claims (Office Action, p. 2-4).

As discussed with respect to Claim 1 above, neither Mitchell nor Waters disclose employing a charging terminal to initiate a charge via account information that was retrieved from a database via biometric information as claimed.

**Regarding Claim 46,** certainly neither Mitchell nor Waters employ preexisting infrastructure to facilitate charging an account based on the account information, wherein the preexisting infrastructure includes a clearing house. Certainly the clearing house of Mitchell must be modified to accommodate biometric information, and consequently, the clearing house does not represent preexisting infrastructure, i.e., infrastructure existing before implementation of Mitchell (e.g., see Mitchell [0023]). Similarly, the merchant payment host 20 of Waters must be modified to handle biometric information before it can be used in the system of Waters (e.g., see Waters [0021]). Such a modified host does not represent preexisting infrastructure, i.e., infrastructure existing before implementation of Waters.

**Regarding Claim 47,** neither the database of Mitchell nor Waters is taught as being positioned remotely from a clearing house, as discussed above.

**Regarding Claim 48,** certainly neither Mitchell nor Waters teach, disclose, or suggest use of a database that independent of a clearing house or bank. Instead, for example, both Waters and Mitchell suggest that the respective databases are maintained by or are included in

a clearing house or host, as discussed above, and that the biometric data contained therein is obtained upon applying for a special account (e.g., Mitchell [0055]; Waters [0018] and [0020]). Certainly neither Mitchell nor Waters disclose a database that operates independently of the operation of a clearing house or bank.

**Regarding Claim 49,** neither Mitchell nor Waters disclose a database that is readily user accessible, where a user can directly edit account information. Instead, financial institutions, such as clearing houses or merchant payment hosts maintain or guard the databases, preventing entry or access by others.

**Regarding Claim 50,** as discussed above, any charging terminals of Mitchell or Waters do not initiate a charge after account information is automatically input thereto.

**Regarding Claims 12-14,** the Office Action suggests (Office Action, p. 7-8) that the combination of Kipp (U.S. Patent No. 5,239,167), Mitchell, and Waters disclose the invention as claimed in Claims 12-14.

Note that Kipp (U.S. Patent No. 5,239,167) does not apparently disclose or suggest disabling of anti-theft features on a tag (e.g., Claim 14). Furthermore, note that the distress signal emitted by a tag of Kipp is not an anti-theft signal, but a distress signal that alerts an employee to a product that may, for example, require manual pricing (as discussed in column 4, lines 39-48 of Kipp). Furthermore, the distress signal is only triggered after the tag is activated at the checkout. A thief is unlikely to pass a checkout line to activate a tag before exiting a merchant outlet.

The combination of Kipp, Mitchell, and Waters would show at most a system for using a biological identifier in place of a credit card number via a terminal that requires navigation of a user interface ([0049]-[0050]), to pay a total determined by Kipp, the transaction of which is initiated by a merchant payment host after authentication of a user. Such a combination would not teach disclose or suggest the invention as claimed and would lack various benefits, including anti-theft provisions, *automatic* checkout, and so on.

The alarm-triggering features disclosed in the present application are adapted to prevent theft of merchandise (Claim 14), which is unlike Kipp, which uses an alarm to notify a user that a product may, for example, require manual pricing (col. 4, lines 39-48 of Kipp). Accordingly, the invention is not obvious in view of the combination of Kipp and Mitchell. Nevertheless, the references should not be combined to reject the Claims, as discussed more fully below.

Mitchell and Waters address different problems than Kipp and should not be combined therewith. The Office Action substantially relies upon such a combination to reject the claims. However, these references take different approaches to solve mutually different problems that are different from the problem addressed by the present invention and contain no suggestion for their combination. Hence, they should not be used alone or in combination to reject the invention as claimed (*In re Wright*, 6 USPQ 2d 1959 (1988)).

In particular, Kipp purportedly discloses a checkout system for wirelessly interrogating randomly disposed articles in a container, while Mitchell discloses a system for authenticating a financial transaction, while Waters purportedly discloses a system for implementing financial transactions using biometric data. Accordingly, Mitchell and Waters address different problems than Kipp, and they should not be combined with Kipp to reject the present invention.

Furthermore the problems addressed by the cited references are different than addressing checkout lines and waits associated with use of cards or complex user interfaces, as addressed by certain embodiments of the present invention.

In addition, the combination of Kipp with Waters and Mitchell represents an unsuggested combination. The references cited do not suggest, expressly or implied, that they be combined to teach the invention as claimed. The references take mutually exclusive paths and reach different solutions to different problems. Hence, they should not be combined as maintained by *In re Wright*, 6 USPQ 2d 1959 (1988). Furthermore, strained interpretations were relied upon to combine the references to reject the claims.

In the above-identified Office Action, the suggestion to combine features from the various references to show the present invention has not come from the prior art references themselves. Prior art references themselves should suggest that they be combined for



rejection of claims under 35 U.S.C. 103, which was forcefully stated, for example, in *In re Sernaker*, 217 U.S.P.Q. 1, 6 (CAFC 1983):

"[P]rior art references in combination do not make an invention obvious unless something in the prior art references would suggest the advantage to be derived from combining their teachings."

This is consistent with the Federal Circuit's suggestion test, which holds that new combinations of old elements (e.g., Kipp and Mitchell) are not obvious unless there is made a specific showing of motivation, suggestion, or teaching to make the combination. See *Teleflex, Inc. v. KSR Int'l Co.*, 119 Fed. App. 282, 285 (Fed. Cir. 2005).

In addition, as forcefully stated, for example in *Heidelberger Druckmaschinen AG v. Hantscho Commercial Prods., Inc.*, 21 F.3d 1068, 1072, 30 USPQ2d 1377, 1379 (Fed. Cir. 1994), determination of obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention. There must be a teaching or suggestion within the prior art, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources of information, to select particular elements, and to combine them in the way they were combined by the inventor.

The notion that the prior art must provide a suggestion or motivation to make such a combination (e.g., Kipp with Mitchell and Waters) for rejection of the claims is further supported by *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 935, 15 USPQ2d 1321, 1324 (Fed. Cir. 1990) and *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985).

The system of Kipp is a stand alone system that is individually complete. It is unclear how Kipp should be modified for use with the system of Mitchell. Such a combination would likely require special hardware and/or software (to interface the systems) that is not taught or suggested in the art. Accordingly, the combination of Mitchell and Kipp would be unobvious.

Furthermore, if it were obvious to couple a system for wirelessly interrogating product tags with a system that enables automated payment via biometric information, then surely it would have been done due to the significant advantages afforded thereby as discussed more fully below.

While use of Kipp may expedite checkout in certain applications, one of the most time consuming tasks, i.e., paying for the merchandise, is not addressed by Kipp, and Mitchell requires potentially slow and cumbersome interaction with a relatively complicated user interface. Accordingly, combination of Kipp with the teachings of the invention as claimed is not obvious. Otherwise, such a combination would surely have been made due to the virtual elimination of checkout lines that would result.

Such a result represents a synergistic benefit, since any reduction in or elimination of an individual user's time spent paying for merchandise translates into time savings for all customers in line. The elimination of the line results in additional significant, potentially unexpected or previously unanticipated results, namely, more customers will likely be attracted to merchants that do not have lines, thereby increasing merchant business. Such synergistic benefits suggest that the invention as claimed is not obvious.

Furthermore, the invention of Mitchell would theoretically require modifying a preexisting charging terminal or card reader (Fig. 1 of Mitchell) to be able to send biometric data to a clearing house. This is unlike certain embodiments of the present invention, which may be adapted for use with preexisting charging terminals, and hence, may more readily work with existing infrastructure.

### **Unexpected Results And Significant Advantages**

Note that in *In re Wiechert*, 370 F.2d 927, 152 USPQ 247 (CCPA 1967), a significant improvement over the related art was held sufficient to rebut prima facie obviousness based on close structural similarity. The present invention provides a marked improvement over the references cited or combinations thereof, as discussed more fully below. Such improvement or advantage may be illustrated by direct or indirect comparison with the closest prior art, as provided above, as suggested *In re Boesch*, 617 F.2d 272, 205 USPQ 215 (CCPA 1980) and

MPEP 716.02(d) - 716.02(e). Hence, Applicants' following comparisons of the present invention with the art of record should be sufficient to establish unexpected properties

As set forth above, various claimed embodiments are unobvious and encompass embodiments with several key advantages over the art of record. For example, certain embodiments afford the ability to use existing infrastructure, such as a clearing house and/or charging terminal, with little or no modification made thereto, and to use biometric information to input an account number to the preexisting infrastructure. Such advantages weigh in favor of patentability, as discussed more fully in Applicant's Amendment C (e.g., pages 26-33 thereof). Advantages of the invention as claimed over Mitchell may be found with reference to Applicant's previous Amendments B-D.

**Regarding Waters**, note that while Waters purportedly suggests transferring an account number to a payment device (e.g., Waters [0022]), the payment device of Waters does not initiate charging in response to the receipt of the number. Instead, Waters requires a subsequent authentication process, implemented by the merchant payment host 20, and the merchant payment host essentially initiates charging the account via the banking network 30 (e.g., Waters [0023]). Accordingly, the merchant payment host 20 initiates the transaction after biometric authentication. Waters essentially transmits the account message back to the payment device 18 to enable the user to accept or decline the transaction (e.g., Waters [0022]). This represents an additional step, which is obviated by the invention as claimed, the invention therefore being further unobvious in view of Waters or Mitchell.

Note that Waters requires additional signaling between the payment device 18 and the merchant payment host 20. This additional signaling may increase network congestion and is highly undesirable and time consuming. The additional signaling will invariably result in additional delays, and may increase shopping lines as the user waits for multiple authentication procedures implemented by the merchant payment host 20 and multiple transfers of biometric information between the payment device 18 and the merchant payment host 20.

Even if the payment device 18 of Waters did initiate charging an account number, such initiation would not occur upon receipt of the account number, but instead would occur only after a user authorizes the transaction, such as by manual (e.g., not automatic) input (e.g.,

Waters [0022]). Clearly, the user in Waters must determine whether to proceed. Accordingly, if the user chooses not to proceed, the transaction will not go forward. Hence, neither Mitchell nor Waters anticipate either alone or in combination the invention as claimed and certainly do not anticipate automatically initiating a charge via a charging terminal in response to receipt of a card number retrieved via use of biometric information.

While Fig. 1 of Waters shows the identity lookup database 24 in a module separate from the merchant payment host 20 or clearing house, the database 24 of Waters is inextricably tied to the operation of the merchant payment host 20 and is certainly not independent or remote thereof (e.g., see Waters [0021]) as claimed (e.g., Claims 3, 24). Similarly, the database of Mitchell is integrated in the clearing house of Mitchell (e.g., Mitchell [0052]; Interview Summary). None of the references teach, disclose, or suggest use of a database that may act separately or remotely from the preexisting clearing houses or merchant payment hosts.

Waters merely provides access to a financial account and does not teach a user-modifiable database. In addition, the database of Waters must be maintained by the merchant payment host and accessed thereby (e.g., see Abstract of Waters), which is highly disadvantageous. Requiring that a merchant payment host or bank maintain biometric information may inhibit wide spread use of the system, as the system of Waters would depend upon acceptance of the system by existing financial institutions. In addition, biometric information of Waters would be proliferated among banks and would not provide user flexibility to edit the behavior of the biometric system.

As discussed in the Summary of Waters, biometric data used to populate the database of Waters must be obtained at the time that the user applies for a financial account with a financial institution, such as a bank (e.g., Waters [0010] p. 2, col. 1, ln. 8-11). This is particularly inefficient when compared to the invention as claimed. For example, if a user believes that his biometric information has been compromised, he must apply for a new account, re-register biometric data, and so on. Similar problems exist with Mitchell. In an embodiment within the scope of the present claims, a user may simply log on to the user-modifiable database and change associations between the biometric information in question and one or more of the user's accounts. For example, if a user has been using a thumb

biometric to access his American Express card account, and he believes that the thumb biometric has been compromised, the user may log on and assign a pointer finger biometric to the American Express card account instead. This can all be done without requiring acceptance of the system by American Express or requiring special financial accounts, and so on, as would be required by Mitchell and Waters.

Hence, certain embodiments of the invention as claimed, which may employ an independent database, provides significant benefits over the art of record. As an additional example, users no longer need to apply or reapply for each credit card, bank card, etc., that they wish to use via biometric information. No special financial accounts are needed. In addition, biometric data is not replicated among multiple financial institutions, where exposure to theft and database break-ins would be increased.

Certainly the database of Waters is not anticipated as being remote, independent of a host or clearing house, or user configurable. Waters certainly does not anticipate retrieving an account number associated with one of a plurality of different financial institutions from a user-accessible database. Instead, in Waters, biometric data is stored at the time that a consumer applies for a financial account with a merchant payment host (e.g., Waters [0018]). In addition, Waters and Mitchell require special financial accounts. For example, in Waters, applying for a financial account is inextricably tied to the obtaining and storing of biometric information, which is highly undesirable (e.g., Waters [0020]) in that it limits a user's ability to configure and adjust the behavior of the system to suit the user's needs.

Recall that in Waters, a user must determine whether to proceed with a given transaction, which suggests that additional user input is required at the point of sale to complete the transaction (e.g., Waters [0022]). This may delay lines and represents a significant disadvantage, which is overcome by the invention as claimed. Certain embodiments according to the invention as claimed do not require user input other than biometric input. The rest of the transaction/charging process may be substantially automatic.

In Waters, a transaction message is transmitted back to the same host that maintains the biometric information, wherein the transaction message is used by the clearing house or host to complete a charge (e.g., Waters [0022]-[0023]).

Further unlike certain embodiments of inventions as claimed (e.g., see Claim 3, 5-10, 15-24, 45, 47), the database of Waters is not an independently accessible database, which may be configured or edited by the user. In certain embodiments of the invention as claimed, the database does not require direct communications with a clearing house, whereas in Waters, the database is integrally tied to the operation of the host and is purportedly involved in sending an EFT signal is sent to a banking network (Waters [0023]). Certain embodiments within the scope of the present claims achieve significant improvements in operational efficiency, configurability, and so on by simply feeding existing infrastructure with an account number retrieved from a remote, user-configurable, independent database.

Note that Waters requires an awkward additional step of comparing biometric information at the host to determine whether an "account unavailable" message should be generated (Waters [0023]). This is highly inefficient and costly to network bandwidth and may further delay shopping lines.

Nowhere does Waters anticipate enabling a user to modify database entries at a point of sale or elsewhere. At most, Waters teaches enabling a user to record information about a transaction that occurred (e.g., Waters [0023]) and to apply for a special biometric financial account (e.g., Waters [0020]). Recording or updating personal records, such as written records, is entirely different than changing biometric associations or changing behaviors in response to the receipt of different biometric information, etc.

Unlike Walters or Mitchell, certain embodiments within the scope of the invention as claimed enable a user to access account numbers stored at a remote repository, i.e., database. Walters instead merely teaches consumer access to a financial account managed by a merchant payment host (e.g., Waters [0024]). This is significantly disadvantageous as compared to the invention as claimed, as detailed above.

Does not use the biometric information to select from plural accounts associated with the same user – e.g., use of the thumb to selectively retrieve different numbers associated with different accounts, e.g. an American Express; use of the index finger to access a MasterCard – all data maintained at the same database.

Note that the system of Walters or Mitchell would require that the user continues to use the same biometric for each transaction. Otherwise, the user may have to proceed with a

potentially lengthy re-application process with the financial institution to obtain another financial account.

Note that the database of Walters must communicate with or be a part of the merchant payment host (Fig. 1 of Walters; [0010]), as detailed above. This is highly disadvantageous, as this would require that the user re-register with different merchant payment hosts, e.g., MasterCard, Visa, American Express, and so on, and would not be applicable to the user's existing accounts, which would have to be modified to work with biometric data. Furthermore, implementation of the system of Waters or Mitchell would require acceptance of the system by each bank or merchant payment host involved, and the biometric information would be undesirably proliferated among multiple banks/hosts.

As an additional example, in a system according to Waters or Mitchell, reorganizing which biometric information is assigned to which card, for all of a user's cards, would require contacting multiple banks, i.e., each bank at which a user maintains a card and associated biometric registration. Furthermore, a user's existing cards could not readily be used with the biometric information unless the associated financial institution accepted the system of Mitchell or Waters, and even then new accounts would need to be opened. This is entirely undesirable and inefficient.

These problems are overcome by retrieving account information to the terminal from a separate database that does not necessarily communicate with a merchant payment host and may be implemented separately therefrom.

**Regarding Waters and Mitchell**, Mitchell generally requires participation of a clearing house and may further require additional manual user input at the point of sale to select from among plural accounts (e.g., Mitchell requires manually pressing "OK" [0050], last sentence, and/or using "controls" [0049]). Similarly, Waters requires participation of a merchant payment host (20 of Fig. 1 of Waters), which must have access to an identity lookup database (24 of Fig. 1 of Waters).

Furthermore, such systems generally lack any functionality or mechanisms that would enable a user to readily change how the system operates, such as to change which accounts are automatically selected in response to different biometric input. Furthermore, both Mitchell

and Waters would require not only acceptance by both a clearing house and/or a merchant payment host, but Mitchell and Waters would require costly modification to existing infrastructure to update the functionality and/or account organization at the clearing house and merchant payment hosts, including credit/charge card companies.

Both Mitchell and Waters require a user to register biometric data when they open a financial account so that appropriate modifications to the infrastructure can be made to handle tokenless biometric-based transactions (e.g., see Mitchell [0024], p. 2, col. 2 and Waters [0010], p. 2, col. 1, ln. 8-14, and [0018], ln. 6-9 thereof). The systems of Mitchell and Waters generally can only be used with special accounts (e.g., Mitchell [0051] and Waters [0020]), and the systems must be accepted by financial institutions for the systems to be implemented. These are significant problems that are overcome by the invention as claimed. These problems arise largely because they do not use separate infrastructure (first means) that provides an account number to preexisting infrastructure via the charging terminal. This negates any suggestion that the invention as claimed is obvious in view of Mitchell and/or Waters.

A brief discussion illustrating additional advantages of certain claimed embodiments follows. A database within the scope of the present claims (e.g., as claimed in Claim 3), including the contents and behavior thereof, is readily modifiable (e.g., online) by a user, for example, to cause the database to return (to the charging terminal) the user's MasterCard number in response to a thumb biometric or to return the user's American Express in response to a pointer finger biometric. In one embodiment, a user may store various account numbers via the database and then selectively change associations between different biometrics and combinations of biometrics by accessing and modifying the database online (e.g., see Claim 8). As another example, if a user believes that his thumb print is being fraudulently used, the user can immediately and easily disable use of the thumb print for a particular credit card and may thereafter use another biometric for that credit card account. A user may assign, via the database, biometrics to any financial account. Financial accounts need not be special biometric accounts as required by the systems of Mitchell and Waters.

Furthermore, unlike Mitchell and Waters, the remote database (e.g., Claim 24) does not require participation or modification of a merchant payment host or a clearing house. A user need not reapply to a bank or credit card company to obtain special biometric-enabled



accounts when they wish to use biometric charging or when they wish to change biometric information (e.g., Mitchell [0055]; Waters [0018]). In addition, wide spread use of certain inventions as claimed does not depend on acceptance thereof by multiple merchant banks and/or clearing houses. Furthermore, sensitive biometric information need not be proliferated among plural databases at different banks around the world (as would obviously occur in the systems of Mitchell and Waters), which would expose the user to increased fraud risk; and costly repetitive modifications to infrastructure represented by merchant payment hosts, clearing houses, and/or databases contained therein to enable the financial infrastructure to use the biometric systems is not required by certain embodiments as claimed.

Both Mitchell and Waters generally teach modifying the operation of existing transaction infrastructure, such as clearing houses, merchant payment hosts, bank accounts, and so on, to enable the infrastructure to use biometric information and communicate with biometric databases to complete a transaction. Unfortunately, such infrastructure modification is undesirable for reasons set forth herein, and information maintained by infrastructure is not readily user editable or modifiable, which is also undesirable. Furthermore, as discussed above, the requisite infrastructure modifications disclosed in Mitchell and Waters would obviously require clearing house, payment host, and bank acceptance before such changes could be made and before Mitchell or Waters could be implemented, which could be prohibitive. Furthermore, in both Mitchell and Waters, a user's biometric information may be undesirably proliferated among banks, clearing houses, and merchant payment hosts, which may increase exposure to fraud.

One embodiment within the scope of the present claims provides a system for facilitating transactions that requires little or no modification to existing clearing houses, financial accounts, e.g., bank or credit card accounts, and so on, and which may readily be adapted for use with existing Point of Sale (POS) terminals and transaction infrastructure, such as clearing houses and bank accounts; does not require proliferation of stored biometric information among clearing houses and banks; does not require acceptance of the invention by banks and clearing houses; and so on. Existing infrastructure (e.g., clearing houses and banks) is currently configured to handle account numbers, such as credit card and charge card numbers, and is not typically configured to handle biometric information to implement

transactions. Accordingly, in one claimed embodiment, biometric information is used to retrieve an account number to the existing infrastructure by delivering the account number to a charging terminal for the purposes thereafter of making a charge via the account number and existing infrastructure (e.g., Claim 1, 22, 45). Consequently, for embodiments constructed according to the present claims, existing infrastructure, such as clearing houses, merchant payment hosts, bank accounts, credit card accounts, and so on, does not require modification, since the infrastructure is already equipped to make charges in response to receipt of an account number.

In a more specific claimed embodiment, the account number is retrieved from a user-modifiable database (e.g., Claims 3, 15, 49) that may be positioned remotely from or act independently from a clearing house. This enables additional benefits. For example, in one implementation falling within the scope of the claims, a user may change biometric information and may change associations between biometric information and financial accounts as needed. For example, if a user believes that someone has acquired his/her thumbprint and is making fraudulent charges, the user may readily disable use of the thumb print and enable use of another biometric (or combination of biometrics), such as pointer-finger print, by accessing the database and making appropriate changes. This advantageous data based configurability is not anticipated by Mitchell and/or Waters.

Existing systems generally do not enable a user to readily access, change, or modify associations (or automatic account selection rules) between biometric information and existing accounts. Generally, the user must apply, such as to MasterCard (e.g., Mitchell [0055]; Waters [0018] and [0020]), to use biometric information to charge a special account (e.g., fingerprint credit card account -- [0051] of Mitchell; Waters [0018]-[0020]). Information associated with any new special accounts, such as fingerprint credit card accounts, must then be propagated through (and proliferated in) the infrastructure so that the clearing house and/or other participating entities (e.g., merchant payment host 20 of Waters, Fig. 1) can appropriately handle the biometric information. Undesirable time consuming proliferation of the biometric information may increase exposure to fraud. Furthermore, unlike the invention as claimed (e.g., Claims 3, 5, 6, 18, 50), account selection in Mitchell or Waters is not automatic. Mitchell generally requires additional user input (which is not

automatic) at a POS terminal, which may delay shopping lines (e.g., [0048]-[0050] of Mitchell). Similarly, Waters must require additional user input to approve or disapprove of a transaction, as discussed in [0022] of Waters. These requirements do not represent automatic retrieval as claimed (e.g., Claim 1).

Furthermore, note that nowhere does Mitchell or Waters disclose or suggest: retrieval of a PIN to a POS based on biometric information for the purposes thereafter of making a charge (e.g., Claim 2); a mechanism that enables a user to control retrieval of account numbers to a POS from a user-modifiable or remote database or any entity (e.g., Claim 4); a mechanism for facilitating prioritizing accounts for automatic retrieval to a POS (e.g., Claim 5) (- use of keys to choose between charge card companies, e.g., [0050] of Mitchell, in no way teaches prioritization or automatic retrieval of a highest priority account); a mechanism that enables a user to specify selection rules based on transaction information (e.g., Claim 8) (- instead, Mitchell merely discloses the notion of associating different biological identifiers with different accounts, which would be manually selected, e.g., [0049]-[0050] of Mitchell)); account selection performed in Mitchell requires manual non-automatic user manipulation of controls (e.g., Mitchell [0049]-[0050]) regardless of whether different finger prints are associated with different accounts (e.g., Claims 3, 5, 6, 18, 50); transmission of a PIN to a clearing house as purportedly suggested in Mitchell is entirely different than employing transaction type information to limit automatic selection of account numbers (e.g., Claim 9); any database taught in Mitchell would not be user-accessible for modification, and Mitchell does not teach use of a user-modifiable database (e.g., Claims 10, 15, 49).

Hence, certain embodiments within the scope of the present claims provide several potentially significant benefits over the art of record. For example, users no longer need to repeatedly interact with a potentially complex user interface when checking out. This expedites checkout lines; obviates the need for users to carry a credit card, ATM card, etc., which are subject to loss or theft; accounts of one's choosing may be selected with different biometric information, thereby obviating the need to carry plural cards to have plural account-charging options, and so on.

As another example, unlike Mitchell and Waters, an embodiment, such as according to Claim 8, might enable a user to automatically charge dinners to one type of card and to charge

SEP 17 2008

Serial No. 10/712,206, Art Unit 2876..... Page 50/51

airfares to another type of card. Alternatively, a user may specify that transactions above a certain dollar amount be charged to one account, and transactions below a certain dollar amount be charged to another account (as discussed, for example, on page 12, lines 16-25 of the present Application). Such functionality may yield additional significant previously unanticipated results in enabling users to organize, categorize, charge, and account for various expenses.

**Request That Subsequent Action Not  
Be Final If New Art Is Cited (per MPEP 706.07(a))**

This amendment did not substantially modify the claims; no new limitations or mechanisms that were not already implied by the present claims or associated record were added. Accordingly, if Examiner cites additional art in the subsequent Office Action, Applicant requests that the action not be made final per MPEP 706.07(a) (§ 3) to enable Applicant time to respond to the additional references. Furthermore, since Applicant is seeking to define Applicant's invention in claims that will give applicant justly entitled patent protection, prosecution should not be prematurely cut off (MPEP 706.07).

**Request per MPEP 707.07(j)**

If Examiner agrees that patentable material exists but does not feel that the present claims are technically adequate, Applicant respectfully requests that Examiner make appropriate suggestions or write acceptable claims pursuant to MPEP 707.07(j).

**Conclusion**

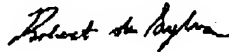
None of the references cited by Examiner taken alone or in combination teaches, discloses, or suggests the invention as presently claimed. For example, none of the references shows a system that can employ biometric information to automatically provide or send an

account number to a charging terminal for subsequently initiating a charge via the charging terminal (e.g., Claim 1, 22, 45). Furthermore, none of the references shows use of a user-modifiable database (e.g., Claim 15). In addition, none of the references shows a database that operates independently of clearing houses, hosts, or other financial institutions (Claim 48).

The present Application is believed to be in proper form for allowance. Accordingly, allowance, and passage to issue are respectfully requested.

I hereby certify that this correspondence is either being transmitted to the United States Patent and Trademark Office at 571-273-8300 or is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450, on September 17, 2008.

Respectfully submitted,



Robert de Sylva (Applicant)

Robert de Sylva,  
161 Ocean Park Blvd. #D  
Santa Monica, CA 90405  
Phone: 310-452-4579